



Ministerium des Inneren, für Digitalisierung und Kommunen
Baden-Württemberg

VIRTUELLE KRIMINALITÄT

Cybercrime



Fotolia

Mit steigender Mediennutzung hat sich ein erheblicher Teil der klassischen Straftaten in den virtuellen Raum verlagert und damit die Modi Operandi vieler herkömmlicher Deliktsformen verändert.

Die digitalisierte Welt ist eine der zentralen Herausforderungen der Kriminalitätsbekämpfung von heute. Durch die über das Internet zur Verfügung stehende digitale Infrastruktur eröffnen sich potenziellen Straftätern neuartige Tatmuster mit enormen Schadensausmaßen für Gesellschaft und Wirtschaft. Nicht nur die Ordnungskriterien wie Zeit und Raum verlieren an Bedeutung, sondern auch klassische Rechtsbegriffe wie Tatort, Tatzeit und örtliche Zuständigkeiten. Cybercrime durchbricht funktionale und territoriale Grenzen und dies in einem hochdynamischen Prozess mit kurzen Innovationszyklen. Vor diesem Hintergrund kommt der Diskussion um die Vorratsdatenspeicherung besondere Bedeutung zu. Je stärker wir uns digital vernetzen, desto mehr nimmt die Verwundbarkeit von Systemen und Usern zu. Begrifflichkeiten wie Bot-Netze, Bitcoins, Cybergrooming, Sexting, Cybermobbing, DDos-Attacken, Identitätsdiebstähle, digitale Schutzgelderpressungen werden immer gebräuchlicher. Es sind

Erscheinungsformen, die zwar in der virtuellen Welt beginnen, ihre schädigende Wirkung entfalten sie jedoch bei jedem einzelnen Opfer, ob in finanzieller Hinsicht oder auch im Hinblick auf die nicht zu unterschätzende psychische Viktimisierung (beispielsweise durch Cybermobbing, Cybergrooming und Sexting).

Vor diesem Hintergrund hat die Polizei Baden-Württemberg einen strategischen Schwerpunkt auf die Bekämpfung von Cybercrime gelegt und umfangreiche präventive und repressive Maßnahmen getroffen, die im Folgenden auszugsweise dargestellt sind:

- Erstellung einer landesweiten Gesamtkonzeption, die im Rahmen eines ganzheitlichen Ansatzes organisatorische und personalplanerische Maßnahmen zur nachhaltigen Bekämpfung des Deliktfeldes Cybercrime festlegt.
- Einrichtung der Abteilung 5 „Cybercrime und Digitale Spuren“ beim LKA BW zum 1. Januar 2012 mit dem Aufgabenspektrum Ermittlungen, anlassunabhängige Internetrecherche, Ansprechstelle Kinderpornographie, IT-Beweissicherung, Ermittlungsunterstützung, Telekommunikationsüberwachung und forensische Datenträgeranalyse.
- Einrichtung von spezialisierten Kriminalinspektionen 5 (Cybercrime, Digitale Spuren) mit kompetenten Ansprechpartnern auf Ebene der regionalen Polizeipräsidien, um das Fachwissen im Bereich der Ermittlungsführung und -unterstützung und bei der Sicherung und Auswertung digitaler Beweismittel (IT-Beweissicherung) zu bündeln.
- Beim LKA BW ist seit Ende 2013 die Zentrale Ansprechstelle Cybercrime (ZAC) eingerichtet. Behörden und Unternehmen, aber auch Bürgerinnen und Bürger haben damit im Kampf gegen Cybercrime einen zentralen Ansprechpartner bei der Polizei. Gerade Wirtschaftsunternehmen sind von IT-Angriffen in hohem Maße betroffen, wenden sich aber nur selten an die Polizei. In diesem Bereich muss nach wie vor von einem erheblichen Dunkelfeld ausgegangen werden.
- Zur professionellen Bekämpfung von Cybercrime wurde zum 1. April 2014 eine beamtenrechtliche Sonderlaufbahn für „Cyberkriminalisten“ eingeführt. Damit können extern ausgebildete Spezialisten in die Laufbahn des Polizeivollzugsdienstes eintreten (1-jährige Ausbildung von Hochschulabsolventen (BA/FH) zum Kriminalkommissar). Im April 2014 konnten die ersten neun Cyberkriminalisten in den Polizeivollzugsdienstes des Landes eingestellt werden.

Link dieser Seite:

<https://im.baden-wuerttemberg.de/de/sicherheit/polizei/kriminalitaetsbekaempfung/cybercrime?print=1&cHash=018a04b7779f5b6f0385a987a1cd1c7f>